UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,267	03/25/2004	Jan Camenisch	CH920020054US1	6902

7590 05/16/2007

LOUIS P. HERZBERG
Intellectual Property Law Dept.
IBM Corporation
P.O. Box 218
Yorktown Heights, NY 10598

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	**PAPER NUMBER**
2109	
MAIL DATE	**DELIVERY MODE**
05/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/809,267	CAMENISCH ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2109	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response of the original filing of March 25, 2004. Claims 1-21 are pending and have been considered below.

Claim Objections

2. Claims 11, 13-21 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claims, or amend the claims to place the claim in proper dependent form, or rewrite the claims in independent form. Claims 11, 13-21 are improperly dependent on claims 1, 5, 7, 9, 10, 12 because: the examiner notes that the applicant is claiming a computer program in claims 11, 13-21 which fail to add, delete, or change any of the steps in the parent claim.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-4, 12-14, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Brennan et al** (US 5675649) in view of **Arditti et al** (US 6125445)

Claims 1, 12-14,21: **Brennan et al** discloses a method for cryptographic key generation comprising:

a. Generating a random secret key (The secret parameters M and x, once generated provided a means of producing a cryptographically secure source of random numbers) (column 11, lines 60-63);

b. Providing a public key comprising an exponent-interval description and a public key value derived from the random secret key, such that the random secret key and a selected exponent value from the exponent interval are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification (M must be a large integer which is the product of two large primes p and q. It is recommended that M have the same number of bit its binary expansion as does N. Absent specific knowledge of p or q. M must be presumed computationally infeasible to factor) (column 10, lines 47-51).

But does not explicitly disclose a step of generating an exponent interval having a first random limit, wherein, with a probability close to certainty, each element of the exponent interval has a unique prime factor that is larger than a given security parameter. However, **Arditti et al** discloses a public key identification process using two has functions, which further disclose a step generating an exponent interval having a first random limit (a parameter m determining the interval [0-m1] in which are drawn the random exponent)(column 4, lines 52-53). Therefore, it would have been obvious

for one having ordinary skill in the art at the time the invention was made to add a step of generating an exponent interval to **Brennan et al**' disclosure. One would have been motivated to generate an exponent interval in order to prevent adversary attack since the security of the system depends on the problem of factoring large number.

Claim 2: **Brennan et al** and **Arditti et al** disclose a method for cryptographic key generation as in claim 1 above, **Brennan et al** further discloses that the step of generating a random secret key comprises using two primes, the product of which is part of the public key (the prime generation algorithm used produced a prime from a subset of all primes in a specific range. In contrast to other methods available for producing cryptographic primes where integers generated are only probable primes. PGEN generates provable primes. Once two primes have been identified by PGEN, they are used to calculate the secret key) (column 12, lines 9-21).

Claim 3: **Brennan et al** and **Arditti et al** disclose a method for cryptographic key generation as in claim 1 above, **Brennan et al** further discloses that the step of generating a random secret key comprises selecting an integer value defining a class group and selecting two elements of the class group (the x^2 mod M random bit generator can converted into a random number generator for producing integers from the interval [a, b]. To pick a number from this interval, random bit sequences of length [1+log2 (b)] bits can be generated until a sequence of bit of bits as a binary number lies in [a, b]) (column 11, lines 37-40).

Claim 4: **Brennan et al** and **Arditti et al** disclose a method for cryptographic key generation as in claim 3 above, **Brennan et al** further discloses that the step of providing a public key comprises computing a modified public key value under use of the selected two elements and the exponent interval (the prime should be selected wisely from a set of all possible primes so that any known cryptographic attack against RSA is foiled) (column 12, lines 6-9).

5. Claims 5, 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Brennan et al** (US 5675649) in view of **Boudot** (Eurocrypt 200, LNCS 1807, pp.431-444, 200).

Claims 5, 15-16: **Brennan et al** discloses a method for cryptographic key generation comprising the steps of:

a. Selecting an exponent value from an exponent interval, wherein each element of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter (M must be a large integer which is the product of two large primes p and q. It is recommended that M have the same number of bit its binary expansion as does N. Absent specific knowledge of p or q. M must be presumed computationally infeasible to factor) (column 10, lines 47-51); and

b. Deriving the signature value from a provided secret key, the selected exponent value, and the message, the signature value being sendable within the network to a second computer node for verification (a third stage comprises creation of a self –signed certificate attesting the certificate authority name, public module N, and public exponent e and the validity period of these public key parameters. A secure hash function is applied to the certificate information to create a message digest, ext the message digest is encrypted with the certificate authority's secret key)(column 12, lines 22-30).

But does not explicitly discloses that the value of the exponent lies in a specific interval. However, **Boudot** discloses an efficient proofs that a committed number lies in an interval, which further discloses a method of publicly verifiable encryption by proving that the committed number belongs to an interval) (section 4). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to set an interval value for the exponent in **Brennan et al**' disclosure. One would have been motivated to do so in order to ensure integrity and authenticity of data and often also confidentiality.

6. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Brennan et al** (US 5675649) in view of **Boudot** (Eurocrypt 200, LNCS 1807, pp.431-444, 200) as applied to claim 5 above, and in further view of **Matyas et al** (US 5265164).

Claim 6: **Brennan et al** and **Boudot** disclose a method for cryptographic key generation as in claim 5 above, but does not explicitly disclose that the step of deriving the signature value further comprises a computation of the i-th root of a value derived from the message and the secret key using a cryptographic hash function, the i being the exponent value. However, **Matyas et al** discloses a method for providing a secure hash and sign signature, which further discloses the step of deriving the signature value further comprises a computation of the i-th root of a value derived from the message and the secret key using a cryptographic hash function (at step 224, the encrypted CFBDKB (i.e., ECFBDKB) is decrypted with the public key algorithm using PRAb, the private device authentication key of device B. PRAb is stored in the CF Environment 146' of the CF 30', and hence is available for use by the ICFER instruction. For example, if the public key algorithm is the RSA algorithm, then decryption consists of raising the ECFBDKB to the power of an exponent d modulo a modulus n, where d and n constitute the private key) (column 37, lines 14-23). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of generating the signature by computing the i-th root to **Brennan et al**' disclosure. One would have been motivated to do so in order to ensure integrity and authenticity of data and often also confidentiality.

7. Claims 7-8, 10, 17-18, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Chaum** (US 4996711) in view of **Boudot** (Eurocrypt 200, LNCS 1807, pp.431-444, 200).

8. Claims 7, 10, 17-18, 20: **Chaum** discloses a selected exponent signature method comprising:

a. Receiving the signature value from a first computer node (This root is communicated to the second party's processor 1208 via a suitable communication link)(column 20, lines 40-43); and

b. Verifying whether an exponent value is contained in an exponent interval, wherein each element of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter, the signature value is invalid if the exponent value is not contained in the exponent interval (the data processor means 1202 of a first party in conjunction with associated means 1204 is capable of determining an exponent from a first message using a procedure known to the first party and to a second party, the exponent containing at least one prime factor uniquely determined by the message. In addition, processor 1202 in conjunction with associated means 1206 is capable of forming a root on a constant known to both first and second parties, said root corresponding to the exponent. This root is communicated to the second party's processor 1208 via a suitable communication link (indicated by dotted lines in FIG. 12). Then processor 1208 in conjunction with associated means 1210 checks the received root by computing the exponent, raising the root to said exponent to produce a result and then verifying that the result is said constant) (column 20, lines 31-46).

But does not explicitly discloses that the value of the exponent lies in a specific interval. However, **Boudot** discloses an efficient proofs that a committed number lies in an interval, which further discloses a method of publicly verifiable encryption by proving that the committed number belongs to an interval) (section 4). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to set an interval value for the exponent. One would have been motivated to do so in order to ensure integrity and authenticity of data and often also confidentiality.

Claim 8: **Chaum** and **Boudot** disclose a method of producing a secure hash and sign signature as in claim 7 above, and **Chaum** further discloses that the step of verifying further comprises a computing step of raising a computed signature root value that being part of the signature value to the power of the exponent value (then processor 1208 in conjunction with associated means 1210 checks the received root by computing the exponent, raising the root to said exponent to produce a result and then verifying that the result is said constant) (column 20, lines 43-46).

9. Claims 9, 11, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Hopkins et al** (US 2003/0120931) in view of **Boudot** (Eurocrypt 200, LNCS 1807, pp.431-444, 200).

10. Claims 9, 11, 19: **Hopkins** discloses a method of producing a secure hash and sign signature comprising:

a. Means for selecting an exponent value from an exponent interval, wherein each element of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter (In accordance with one aspect of the present invention, the of the individual private keys includes: an associated individual modulus n.sub.i that is a number formed as a product of one or more of the k prime factors of the group modulus n; and an associated individual private exponent d.sub.i that is determined based on a selected public group exponent e, and also based on the prime factors of the associated individual modulus n.sub.i. Each of the individual private exponents d.sub.i may be determined as a number congruent to the inverse of the public group exponent e, modulo the Euler Totient function of the associated individual modulus n.sub.i)(page 2, paragraph 18); and

b. Means for deriving the signature value from a provided secret key, the selected exponent value, and the message, the signature value being sendable within the network to a second computer node for verification (Creation of a digital signature usually includes deriving a hash value of the message to be signed and then performing a mathematical operation on that value using the private key. Typically, the digital signature is attached to the corresponding message and transmitted to a second party) (page 1, paragraph 9).

But does not explicitly discloses that the value of the exponent lies in a specific interval. However, **Boudot** discloses an efficient proofs that a committed number lies in an interval, which further discloses a method of publicly verifiable encryption by proving

that the committed number belongs to an interval) (section 4). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to set an interval value for the exponent. One would have been motivated to do so in order to ensure integrity and authenticity of data and often also confidentiality.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kocher et al: (US 6381699) Leak-resistant cryptographic method and apparatus

b. Ishii: (US 5768389) Method and system for generation and management of secret key of public key cryptosystem.

c. Leighton et al: (US 5519778) Method for enabling users of a cryptosystem to generate and use a private pair key for enciphering communications between the users.

d. Chaum: (US 4949389) Returned value blind signature system.

e. Shamir: (US 4933970) Variants of the flat-schamir identification and signature scheme.

f. Leighton: (US 5647000) Failsafe key escrow system.

g. Gennaro et al (US 6578144) Secure hash and sign signature.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:30 a.m. to 4:30 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jim W. Myhre, can be reached on (571) 272 6722. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 274-1685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Monday, May 7, 2007

James W. Myhre
Supervisory Patent Examiner